KOFETKE.

26 / 30

VODNIKI O AI

Ločevanje strank v enem delovnem toku z AI

Kako se lahko skupna orodja izognejo mešanju zaupnih projektov?



LOČEVANJE STRANK

Zemljevid toka podatkov in preverjanja izolacije za majhno storitveno podjetje.

BRALNA IZDAJA

september 2026
Lokalna izdaja · september 2026

Viri preverjeni 23. septembra 2026.

Majhno storitveno podjetje pogosto želi en uporaben delovni tok z AI, ne ločenega sklopa programske opreme za vsako stranko. Isti pomočnik lahko pripravi osnutek zapiskov sestanka, razvršča prejete datoteke, sestavi posodobitev projekta in išče po preteklem delu. Priročnost je resnična. Resnično je tudi tveganje: uporaben odgovor za stranko A lahko postane kršitev zaupnosti, če črpa iz gradiva stranke B.

Tveganja praviloma ne reši že to, da mapo poimenujemo po stranki. Ločevanje strank mora preživeti celotno pot informacije: nalaganje, izvlek besedila, indeks, navodilo modelu, klic orodja, izhod, dnevnik, predpomnilnik, varnostno kopijo in človeški pregled. Oznaka stranke, ki izgine po prvem koraku, je okrasek, ne izolacija.

Članek opisuje sorazmerno zasnovo za izmišljeno majhno storitveno podjetje. Ne gre za recept za certifikacijo ali pravno presojo. Namen je, da lastnik lahko preveri, ali skupni delovni tok projekte dejansko drži narazen.

Začnite z zemljevidom toka podatkov

Vzemimo izmišljeni oblikovalski studio Northline Studio. Ima tri stranke in pomočnika uporablja za iskanje po projektih ter prve osnutke posodobitev stanja. Pred izbiro modela studio nariše pot ene datoteke stranke:

```
Nalaganje stranke
     |
[client_id + project_id + razred dostopa]
     |
Izvlek besedila --> indeks za posamezno stranko
     |                    |
     +--> odobreno orodje
               |
          odgovor s povezavami do virov
               |
          evidenca dejavnosti
```

Diagram je namenoma nepopoln. Ekipo vodi do vprašanj: Kje je izvirna datoteka? Ali izvlečeno besedilo ohrani isti **client_id**? Ali lahko iskalna poizvedba seže v indeks druge stranke? Ali predpomnjeni odgovor ponovi isti pregled dostopa? Kdo sme videti evidenco dejavnosti?

NIST SP 800-53 razlikuje nadzor toka informacij od navadnega nadzora dostopa. Kontrola AC-4 zahteva uveljavljanje odobrenih pooblastil za tok informacij v sistemu in med povezanimi sistemi na podlagi določenih politik.[1] Majhnemu studiu ni treba uvesti obsežnega državnega kataloga kontrol. Uporabno načelo je preprosto: ne odločajte le o tem, *kdo lahko odpre datoteko*, ampak tudi *kam sme njena vsebina potovati naprej*.

Identiteta stranke je zahteva, ne namig

Vsak predmet, ki vstopi v delovni tok, potrebuje zanesljivo vrednost meje. V izmišljenem studiu je to **client_id**; projekt lahko doda **project_id**. Sistem ju dobi iz nadzorovanega registra strank in projektov ali iz izbire preverjenega delovnega prostora, ne iz ugibanja pomočnika o imenu, omenjenem v dokumentu.

Varen notranji zahtevek ima mejo pripeto še pred začetkom iskanja:

```
requester_id: user-041
client_id: CL-NEVA
project_id: PR-118
purpose: draft weekly project update
allowed_actions: search_project, read_approved_files,
create_draft
```

Pomočnik lahko zahtevek prejme kot kontekst, vendar ga mora aplikacija uveljaviti. Jezikovni model lahko ponovi **client_id: CL-NEVA**, pa kljub temu zahteva napačne podatke, če iskalno orodje sprejme neomejeno poizvedbo. Orodje mora zavrniti zahtevek brez veljavne meje stranke in to mejo na strežniški strani uporabiti pri izbiri datotek, indeksov in povezanih storitev.

NIST-ova arhitektura ničelnega zaupanja ponuja uporaben odnos do problema: za sredstva ali račune ni samodejnega zaupanja samo zaradi lokacije v omrežju ali lastništva; preverjanje istovetnosti in pooblastila se opravita pred vzpostavitvijo seje do vira podjetja.[2] Pri skupnem pomočniku prijava uporabnika ni dovolj. Sistem mora odločiti, ali sme ta uporabnik zdaj opraviti to dejanje nad gradivom te stranke.

Mejo ohranite v vsaki shrambi

Pogosta šibka zasnova ima ločene mape, vendar en skupni indeks za pridobivanje informacij. Besedilo vsake stranke se pretvori v vektorske predstavitve ali kopira v isto zbirko, iskalna poizvedba pa vpraša po »nedavnih težavah z dostavo«. Najbližji rezultat je lahko od napačne stranke. Vodja projekta nato vidi verjeten odstavek, iz katerega je povzetek izpustil ime stranke. To je vrsta napake, ki je na predstavitvi videti sposobna, v običajnem delu pa ni sprejemljiva.

Pogosti sta dve zasnovi:

Vzorec

Ločen delovni prostor ali indeks za vsako stranko

Meja	Fizična ali logična shramba se izbere pred pridobivanjem
Prednost	Lažje razumljivo; poizvedba ima manj mest za iskanje
Napaka, ki jo je treba preizkusiti	Orodje po nesreči poizveduje po vseh delovnih prostorih; skupni predpomnilnik vrne star odgovor

Skupna shramba z obveznim filtrom stranke

Meja	Vsak zapis in poizvedba nosita **client_id**; politika zbirke podatkov ga uveljavlja
Prednost	Pri mnogih majhnih strankah je lahko gospodarna
Napaka, ki jo je treba preizkusiti	Razvijalec pozabi en filter; skrbnik uporabi širok izvoz; vektorsko iskanje obide politiko

Noben vzorec ni varen samo zato, ker je narisan v diagramu. Pomemben preizkus je, ali zahtevek z **CL-NEVA** lahko pridobi, izvozi, povzame ali citira predmet iz **CL-ORIS**. Če je odgovor »samo če se razvijalec spomni filtra«, je meja šibka.

Isto pravilo velja za izpeljano gradivo. Kos besedila, vektorska predstavitev, ustvarjen povzetek, predogled priloge in vnos v predpomnilniku niso neškodljivi zato, ker niso izvirni PDF. Lahko razkrijejo iste zaupne informacije. Izpeljanemu gradivu dajte izvorni **client_id**, identifikator vira in razred dostopa. Povzetka ne kopirajte v splošno zbirko »uporabnega znanja«, dokler zavesten pregled ne odloči, da je lahko deljen.

Pomočnik naj pove svoj obseg

Skupni delovni tok je lažje pregledati, kadar vsak odgovor navede obseg, ki ga je uporabil. Northlinov osnutek posodobitve se lahko začne z internim zaglavjem:

```
Obseg: CL-NEVA / PR-118
Preiskani viri: 14 potrjenih projektnih datotek
Izključeno: druge stranke; zasebna kadrovska mapa; neodobreni osnutki
Vrsta rezultata: osnutek za pregled vodje projekta
```

To samo po sebi ni varnostna ovira. Je preverljiva trditev. Če pregledovalec vidi vir iz **CL-ORIS**, je napaka vidna, preden osnutek zapusti studio.

Uporabno pravilo za izhod je: brez povezave do vira ni dejanske trditve o stranki. Pomočnik lahko napiše predlagani stavek, vendar naj ga označi kot osnutek brez vira. To nadaljuje razlikovanje med delovnim zapiskom in verodostojnim zapisom. Uglajena posodobitev stanja je še vedno le osnutek, dokler lastnik projekta ne pregleda navedenega gradiva in ne odobri sporočila.

Dovoljenje je več kot meja stranke

Ločevanje strank ne pomeni, da lahko vsak zaposleni vidi vsak predmet pri dodeljeni stranki. Vodja projekta morda potrebuje projektne briefinge, ne pa plačilnih podatkov. Računovodja morda potrebuje račune, ne pa dokumentov o strategiji izdelka. Zunanji sodelavec morda potrebuje opis naloge, ne pa celotnega skupnega diska.

Uporabite dva pregleda skupaj:

1. **Pregled meje:** ali se zahtevek ujema s pravo stranko in projektom?
2. **Pregled vloge in namena:** ali sme ta prosilec opraviti to dejanje nad tem razredom gradiva za navedeni namen?

Kontrola AC-3 v NIST SP 800-53 zahteva odobrena pooblastila za logični dostop do informacij in sistemskih virov v skladu s politikami nadzora dostopa.[1] To je znova oblikovalsko merilo in ne trditev, da mora slovensko podjetje prevzeti besedilo NIST-ovih kontrol. Praktična posledica pa je, da je splošna vloga »član ekipe« pri skupnem delovnem toku AI pogosto preširoka.

GDPR pri osebnih podatkih zahteva ukrepe varnosti, primerne tveganju, med drugim po potrebi sposobnost zagotavljanja stalne zaupnosti, celovitosti, razpoložljivosti in odpornosti sistemov ter storitev obdelave.[3] Uvodna izjava 84 kot tveganje obdelave navaja nepooblaščeno razkritje osebnih podatkov, ki se prenašajo, hranijo ali drugače obdelujejo, oziroma dostop do njih.[3] Ti določbi ne predpisujeta posamezne vektorske zbirke, ponudnika identitet ali oblike navodila modelu. Težko pa podpreta zasnovo, v kateri je pridobivanje podatkov med strankami običajna funkcija.

Izmišljen primer napake

Northline dokumente vsake stranke hrani v različnih mapah v oblaku. Da bi bilo iskanje hitro, zunanji sodelavec čez noč zgradi en združen indeks besedil. Orodje za poizvedbe sprejme parameter **client_id**, vendar ga doda le kot besedno zvezo navodilu modelu; zapisov dejansko ne filtrira.

Vodja projekta Neva vpraša: »Kateri datum dostave je trenutno ogrožen?« Pomočnik najde podobno težavo pri Oris, prepiše povzetek brez imena stranke in vrne 16. oktober. Vodja projekta pošlje posodobitev, preden preveri povezavo do vira. Napačen datum je zdaj v e-pošti, delovni tok pa je razkril tudi obstoj težave z dostavo druge stranke.

To bi ustavili številni zaščitni ukrepi:

- indeksator bi **client_id** hranil kot obvezen metapodatek iz nadzorovanega registra;

- pridobivanje bi zahtevalo natančen strežniški filter in vrnilo nič rezultatov, če filter manjka;
- izhod bi prikazal identifikator vira in obseg stranke; ter
- preskus bi uporabljal namenoma podobne dokumente različnih izmišljenih strank.

Pripravljenosti modela, da sledi navodilu, ne obravnavajte kot enega od teh ukrepov. To je uporabno vedenje, ne uveljavljanje pravil.

Evidenca dejavnosti brez arhiva nadzora ljudi

Ko gre nekaj narobe, podjetje potrebuje dovolj dokazov za preiskavo. Evidenca dejavnosti lahko vsebuje identifikator zahtevka, prosilca, dejanje, mejo stranke in projekta, izbrane identifikatorje virov, izid odločitve ter časovni žig. Običajno ne potrebuje celotne vsebine dokumentov ali popolnega prepisa navodila.

Na primer:

```
event_id: EVT-20260923-184
requester_id: user-041
client_id: CL-NEVA
project_id: PR-118
action: search_project
source_ids: [DOC-118-07, DOC-118-11]
outcome: allowed
review_flag: false
```

NIST-ov Okvir za zasebnost povezuje upravljanje tveganj za zasebnost s poslovnimi razlogi, organizacijskimi vlogami in odgovornostmi ter dejavnostmi za zaščito zasebnosti.[4] To podpira praktično vprašanje za studio: kdo odloči o hrambi evidenc dejavnosti, kdo jih sme pregledati in kdaj se odstranijo? Zapis, ki pomaga preiskati dostop med strankami, lahko sam razkrije osebne ali poslovno občutljive podatke, če se široko kopira ali hrani brez konca.

Načelo najmanjšega obsega podatkov v GDPR pravi, da morajo biti osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namen obdelave.[3] V tem okviru je to razlog za beleženje identifikatorjev in izidov, ne vsake zaupne povedi, ki jo je uporabnik vnesel. Roki hrambe in pravne obveznosti so različni, zato naj jih podjetje določi z ustreznim nasvetom, ne z univerzalno številko iz tega članka.

Preverjanja izolacije, ki jih majhno podjetje res lahko izvede

Preizkušanje naj bo nasprotovalno, vendar neškodljivo. Uporabite izmišljene dokumente, ne datotek strank. Ustvarite dva majhna projekta s podobnimi dejstvi: oba imata »zamudo pri dostavi«, oba omenjata »Fazo 2«, v vsakem pa je drugačna cena. Preizkuševalcu dodelite le vlogo ene stranke.

Te preglede opravite po pomembni spremembi delovnega toka in občasno tudi sicer:

Preverjanje	Pričakovani izid	Dokaz, ki ga hranite
Iskanje s pravo stranko in projektom	Pojavijo se le viri iz tega obsega	Vrnjeni identifikatorji virov in vrednosti meje
Iskanje brez `client_id`	Zahtevek se varno zavrne; ni širokega nadomestnega iskanja	Dogodek zavrnitve
Iskanje z natančnim identifikatorjem druge stranke	Ni rezultata ali je dostop zavrnjen	Zapis preizkusa in izhod
Ponovljen predpomnjeni odgovor po odvzemu dovoljenja	Predpomnilnik se ne vrne; pooblastilo se preveri znova	Dogodek zavrnitve ali ponovne preveritve
Izvoz ali klic povezanega orodja	Veljajo ista preverjanja meje in vloge	Evidenca dejavnosti orodja

Kratek izračun lahko pokaže, ali se preverjanja dejansko izvajajo. Če načrtovan niz obsega 12 zahtevanih preverjanj in jih je 11 izvedenih z zabeleženim izidom, je pokritost 11 / 12 = 0,9167 oziroma 91,67 %. To je pokritost načrtovanih pregledov, ne dokaz, da delovni tok nima uhajanja. Manjkajoči pregled si še vedno zasluži pozornost, zlasti če zadeva predpomnilnik ali zunanji priključek.

NIST-ova publikacija o ničelnem zaupanju opredeljuje ničelno zaupanje kot pristop, ki skuša zmanjšati negotovost pri uveljavljanju natančnih odločitev o dostopu z najmanjšimi pravicami za vsak zahtevek, tudi v omrežju, ki ga obravnavamo

kot ogroženo.[2] Za majhno podjetje je uporaben izraz »za vsak zahtevek«. Preverjanje dovoljenja ob prijavi ne zaščiti samodejno poznejšega pridobivanja, izvoza ali predpomnjenega odgovora.

Kaj skupna infrastruktura pomeni in česa ne

Skupna infrastruktura sama po sebi ni neuspeh zasebnosti. Podjetje lahko uporablja en sistem identitete, eno storitev zbirke podatkov, enega ponudnika modela ali eno storitev nadzora, medtem ko meje strank uveljavlja z ločenimi delovnimi prostori, šifrirnimi ključi, politikami najemnikov in pregledi v aplikaciji. Zasnova mora pokazati, kje se ti pregledi opravijo in kdo jih lahko preglasi.

Nasprotno ločene mape same po sebi niso izolacija. Če lahko skupni skrbniški račun množično izvozi vse datoteke, če ima žeton avtomatizacije širše pravice kot oseba, ki ga uporablja, ali če indeks vektorskih predstavitev ne upošteva metapodatkov o dostopu, delovni tok še vedno lahko pomeša projekte. Poverilnice, opravila v ozadju, dnevnike, predpomnilnike in dostop podpore ponudnika obravnavajte kot dele istega toka podatkov.

Zasnova mora preživeti tudi običajno človeško napako. Uporabnik lahko v spustnem seznamu izbere napačno stranko. Oseba lahko v klepet prilepi ime stranke, ne da bi pripela projekt. Dokument dobavitelja lahko omenja dve stranki. Varen odziv ni samozavestno ugibanje. Je zahteva po potrjeni meji ali jasno omejen rezultat.

Kratko pravilo delovanja

Northline lahko pravilo pove v običajnem jeziku:

> Vsako dejanje za stranko ali iz gradiva stranke mora od vnosa do izhoda nositi preverjeno mejo stranke. Sistem zavrne manjkajočo ali nasprotujočo mejo, jo uporabi pri iskanju, orodjih, predpomnilnikih in dnevnikih ter pregledovalcu pokaže identifikatorje virov, potrebne za preverjanje rezultata.

To pravilo ne nadomešča pogodb, nasveta glede varstva podatkov ali tehničnega preizkušanja. Je preverljiva obljuba. Skupni pomočnik postane obvladljiv, ko podjetje lahko pokaže meje, jih poskuša z neškodljivimi testnimi podatki prekiniti in natančno vidi, kaj se je zgodilo ob zavrnitvi zahtevka.

Viri

Številke virov veljajo za ta vodnik. Povezave vodijo do izvirnih dokumentov. Pred uporabo preverite besedilo, pogoje uporabe in razpoložljivost storitev.

[1] **NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*.**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[2] **NIST SP 800-207, *Zero Trust Architecture*.**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[3] **Regulation (EU) 2016/679, *General Data Protection Regulation*, Article 5, Article 32 and Recital 84.**
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[4] **NIST, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*.**
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf